TORSION OF RATIONAL ELLIPTIC CURVES OVER CUBIC FIELDS AND SPORADIC POINTS ON $X_1(n)$

FILIP NAJMAN

Abstract. We classify the possible torsion structures of rational elliptic curves over cubic fields. Along the way we find a previously unknown torsion structure over a cubic field, $\mathbb{Z}/21\mathbb{Z}$, which corresponds to a sporadic point on $X_1(21)$ of degree 3, which is the lowest possible degree of a sporadic point on a modular curve $X_1(n)$.

1. Introduction

When trying to understand elliptic curves over number fields, an important problem is to classify the possible torsion structures. The first such classification was done by Mazur [23, 24], proving that the torsion of an elliptic curve over $\mathbb{Q}$ has to be isomorphic to one of the following 15 groups:

$$\begin{gathered}\mathbb{Z}/m\mathbb{Z}, 1 \leq m \leq 12,\ m \neq 11,\\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z},\ 1 \leq m \leq 4.\end{gathered} \tag{1}$$

After this result, attention shifted toward number fields. Kamienny [14] proved that if a torsion point of an elliptic curve over a quadratic field has prime order p, then $p \leq 13$. This, when combined with a theorem of Kenku and Momose [20], gave a complete list of possible torsion structures over quadratic fields:

$$\begin{gathered}\mathbb{Z}/m\mathbb{Z}, 1 \leq m \leq 18,\ m \neq 17,\\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z},\ 1 \leq m \leq 6,\\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z},\ m = 1, 2,\\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.\end{gathered} \tag{2}$$

The author gave a similar complete list for the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ (see [30]), and a procedure how to make such a list was developed by Kamienny and the author [15].

As one can see, much is known about the possible torsion structures of elliptic curves over $\mathbb{Q}$ and over quadratic fields. Unfortunately, already over cubic fields a classification of possible torsion structures of elliptic curves is not known. However, it is known that if an elliptic curve over a cubic field

2000 *Mathematics Subject Classification.* 11G05, 11G18.

Key words and phrases. Elliptic curves, torsion subgroups, cubic fields, modular curves.

The author was supported by the Ministry of Science, Education, and Sports, Republic of Croatia, grant 037-0372781-2821.

has a point of prime order p, then $p \leq 13$ (see [33, 34]). Jeon, Kim and Schweizer [12] found all the torsion structures that appear infinitely often as one runs through all elliptic curves over all cubic fields:

$$\begin{gathered} \mathbb{Z}/m\mathbb{Z}, 1 \leq m \leq 20,\ m \neq 17, 19, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z},\ 1 \leq m \leq 7. \end{gathered} \tag{3}$$

Jeon, Kim and Lee [10] constructed infinite families having each of the torsion structures from the list (3).

However, it was unknown whether the list (3) is complete, i.e. if one runs through all elliptic curves over all cubic fields, do there exist torsion structures that appear only finitely many times? We show, by finding an elliptic curve with torsion $\mathbb{Z}/21\mathbb{Z}$ over a cubic field, that the answer is yes and that the list (3) is not the complete list of possible torsion structures over cubic fields.

The main purpose of this paper is to study the possible torsion structures of all rational elliptic curves (meaning that all their coefficients are $\mathbb{Q}$-rational) over all cubic fields. This is a natural question to consider as, apart from being interesting in itself, it is often important to study rational elliptic curves over extensions of $\mathbb{Q}$ when solving Diophantine equations (see for example [2]).

The main result of this paper is the following theorem.

Theorem 1. *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a cubic extension. Then $E(K)_{tors}$ is one of the following groups*

$$\begin{gathered} \mathbb{Z}/m\mathbb{Z},\ m = 1, \ldots, 10, 12, 13, 14, 18, 21, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z},\ m = 1, 2, 3, 4, 7. \end{gathered} \tag{4}$$

The elliptic curve $162B1$ over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve over a cubic field with torsion $\mathbb{Z}/21\mathbb{Z}$. For all the other groups T in the list (4), there exists infinitely many rational elliptic curves that have torsion T over some cubic field.

To prove Theorem 1, we will first need to solve the analogous problem for quadratic fields, which we do in Section 3.

We prove Theorem 1 by studying the action of the Galois group on the torsion points, division polynomials, and by finding the rational points on certain (modular) curves.

Let us mention that a somewhat similar problem to the one considered in this paper is the problem of finding the possible torsion structures of rational elliptic curves with integral j-invariant [29, 35] and with complex multiplication over number fields [5, 3].

Recall that the *gonality* $\gamma(X)$ of an algebraic curve X is the lowest degree of a nonconstant rational map from X to the projective line. We call points of degree d on the modular curves $Y_1(m, n)$ (see Section 2 for definitions of modular curves and note that we only consider modular curves with $m = 1, 2$ in this paper), when $d < \gamma(Y_1(m, n))$ *sporadic*. Since all the

modular curves $Y_1(m,n)$ that correspond to the torsion structures in the list(1) are of genus 0 and have (infinitely many) rational points (since some of the cusps of $X_1(m,n)$ are rational) and hence are of gonality 1. Similarly, all the modular curves $Y_1(m,n)$ that correspond to the torsion structures in the list (2) are of genus ≤ 2 (and hence have gonality 1 or 2), so it follows that there are no sporadic points of degree 1 or 2. Van Hoeij [36] found sporadic points of degree 6 on $X_1(37)$ (of gonality 18), and of degree 9 on $X_1(29)$ and $X_1(31)$ (of gonality 11 and 12, respectively).

The unique rational elliptic curve with 21-torsion over a cubic field hence gives us a degree 3 sporadic point, which is the lowest degree possible. By the method used to construct this point we rediscover van Hoeij's degree 6 point on $X_1(37)$.

2. Conventions and notation

Throughout this paper, K will be a cubic field and L will be its normal closure over $\mathbb{Q}$. This means that when $K/\mathbb{Q}$ is normal, then $L = K$, and otherwise L is a degree 6 extension of $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$. We denote by M the unique field with the property that M is a subfield of L such that $[L : M] = 3$ (from which it follows that $\mathrm{Gal}(L/M) \simeq \mathbb{Z}/3\mathbb{Z}$). If K is normal over $\mathbb{Q}$, this will mean that $M = \mathbb{Q}$.

Let $E[n] = \{P \in E(\overline{\mathbb{Q}}) | nP = 0\}$ denote the n-th division group of E over $\overline{\mathbb{Q}}$ and let $\mathbb{Q}(E[n])$ be the n-th division field of E.

We will denote by E^d a quadratic twist of E by $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. By ζ_n we will denote a nth primitive root of unity and by $\mathbb{Q}(\zeta_n)^+$ the maximal real subfield of $\mathbb{Q}(\zeta_n)$.

We denote by ψ_n the n-th division polynomial of an elliptic curve E (see [37] for details), which satisfies that, for a point $P \in E$, $\psi_n(x(P)) = 0$ if and only if $nP = 0$. As before, although the division polynomial depends on the curve E, we will leave E out of the index as it will be clear what elliptic curve we are referring to. A method we will often use throughout the paper for checking whether a fixed rational elliptic curve E obtains n-torsion over some extension of degree d is to factor ψ_n and then compute what the torsion is in the extensions generated by factors of degree l, where $l|d$. In the special case when $d = 2$ one has to also check for the fields generated by the y-coordinates corresponding to the roots of linear factors of ψ_n. We call this method the *division polynomial method*. Note that the division polynomial method can also be effectively used in determining which, if any, twists of a given curve have n-torsion over the base field.

If there exists a K-rational isogeny $\phi : E \to E'$ of degree n, this implies that $\mathrm{Ker}\,\phi$ is $\mathrm{Gal}(\overline{K}/K)$-invariant cyclic group of order n and we will say that E/K has an n-isogeny.

When counting rational elliptic curves, unless stated otherwise, we will count up to $\mathbb{Q}$-isomorphism. When referring to specific elliptic curves we

will list them as they appear in Cremona's tables [4], as we already did in Theorem 1.

Denote by $Y_1(m,n)$ the affine modular curve whose K-rational points classify isomorphism classes of the triples (E, P_m, P_n), where E is an elliptic curve (over K) and P_m and P_n are torsion points (over K) which generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$. For simplicity, we write $Y_1(n)$ instead of $Y_1(1,n)$. Let $X_1(m,n)$ be the compactification of the curve $Y_1(m,n)$ obtained by adjoining its cusps.

Denote by $Y_0(n)$ the affine curve whose K-rational points classify isomorphism classes of pairs (E,C), where E/K is an elliptic curve and C is a cyclic ($\mathrm{Gal}(\overline{K}/K)$-invariant) subgroup of E. Let $X_0(n)$ be the compactification of $Y_0(n)$.

Recall that a $\mathbb{Q}$-*curve* is an elliptic curve E, such that it is $\overline{\mathbb{Q}}$-isogenuos to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates.

For computations we use Magma [1].

3. Torsion of rational elliptic curves over quadratic fields

The results of this short section will be needed in the proof of Theorem 1, but are also interesting in their own right. They also provide a nice introductory exercise for the much harder cubic fields case.

Theorem 2. *Let E be a rational elliptic curve and F a quadratic field.*

a) *The torsion of $E(F)$ is isomorphic to one of the following groups*

$$\begin{gathered}\mathbb{Z}/m\mathbb{Z},\ m=1,\dots,10,12,15,16\\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2m\mathbb{Z},\ 1\le m\le 6.\\ \mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3m\mathbb{Z},\ m=1,2,\\ \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}.\end{gathered} \tag{5}$$

b) *Each of these groups, except for $\mathbb{Z}/15\mathbb{Z}$, appears as the torsion structure over a quadratic field for infinitely many rational elliptic curves E.*

c) *The elliptic curves $50B1$ and $50A3$ have 15-torsion over $\mathbb{Q}(\sqrt{5})$, $50B2$ and $450B4$ have 15-torsion over $\mathbb{Q}(\sqrt{-15})$. These are the only rational curves having non-trivial 15-torsion over any quadratic field.*

Remark 3.
a) The elliptic curves 50B1 and 50A3 are twists by 5 of each other, and hence become isomorphic over $\mathbb{Q}(\sqrt{5})$. Similarly, 50B2 and 450B4 are twists of each other by -15 and become isomorphic over $\mathbb{Q}(\sqrt{-15})$.
b) These elliptic curves are "exceptional curves", in the sense that they are the only elliptic curves (not just rational) over the respective quadratic fields with 15-torsion (see [15, 31] for details).

Before we proceed with the proof of Theorem 2, we will prove the following lemma.

Lemma 4. *Let E be a rational elliptic curve. Then in the family of all twists E^d of E (including E itself) there is at most one elliptic curve with nontrivial n-torsion for $n = 5, 7$, and at most 2 curves with 3-torsion.*

Proof. It is well known that if $F = \mathbb{Q}(\sqrt{d})$, and n an odd integer then

$$E(F)[n] = E(\mathbb{Q})[n] \oplus E^d(\mathbb{Q})[n]. \tag{6}$$

Thus it follows that $E(\mathbb{Q})$ and $E^d(\mathbb{Q})$ cannot both have n-torsion for $n = 5$ or 7, since an elliptic curve cannot have full n-torsion over a quadratic field.

It is impossible that E has 3 twists with 3-torsion, as this would imply that, by an argument as in (6), $E(F_2)$ would contain $(\mathbb{Z}/3\mathbb{Z})^3$ for some biquadratic F_2 extension of $\mathbb{Q}$. □

Proof of Theorem 2. The possible torsion structures of a rational elliptic curve over a quadratic field is obviously a subset of the list (2). The equality (6) rules out the possibility of n-torsion for $n = 11, 13$. Note that the number of points of order 2 over F on an elliptic curve

$$E : y^2 = f(x) = x^3 + ax + b$$

is equal to the number of roots of f over F. It follows that if $E(\mathbb{Q})$ has no 2-torsion, then neither does $E(F)$. Thus if $E(F)$ had n-torsion, for $n = 14, 18$, it would follow that there exists an elliptic curve with n-torsion over $\mathbb{Q}$, which is impossible.

It can be seen from [11, Theorems 3.7, 3.8., 3.9., 3.10. and 3.11.] that there exist infinitely many rational elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

In [22, Remark 2.6. (d)] one is given a construction which can be used to construct infinitely many rational elliptic curves with 16-torsion over quadratic fields.

Finally, we wish to find all rational elliptic curves with 15-torsion over quadratic fields. Let $E/\mathbb{Q}$ be an elliptic curve which attains 15-torsion over a quadratic field. By (6) this implies that,

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z} \text{ and } E^d(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z} \tag{7}$$

or vice versa. Suppose without loss of generality that it is as in (7). It also follows, since if E has a p-isogeny, so do all the quadratic twists E^d of E, that E has to have a 15-isogeny. But there are only 4 families of twists of rational elliptic curves with a 15-isogeny [27, p.78–80], those with j-invariant

$$-25/2,\ -349938025/8,\ -121945/32,\ 46969655/32768,$$

which are the twists of the elliptic curves 50A1, 50A2, 50B1 and 50B2, respectively.

By the division polynomial method we find that 50B1 has 15-torsion only over $\mathbb{Q}(\sqrt{5})$ and 50B2 has 15-torsion only over $\mathbb{Q}(\sqrt{-15})$, and that 50A1 and 50A2 have no twists with 5-torsion, completing the proof of the theorem. □

4. Auxiliary results

In this section we prove a series of results that we will need for the proof of Theorem 1.

Lemma 5. *Let $F/\mathbb{Q}$ be a quadratic extension, n an odd positive integer, and $E/\mathbb{Q}$ an elliptic curve such that $E(F)$ contains $\mathbb{Z}/n\mathbb{Z}$. Then $E/\mathbb{Q}$ has an n-isogeny.*

Proof. As already mentioned in (6), if $F = \mathbb{Q}(\sqrt{d})$, then

$$E(F)[n] = E(\mathbb{Q})[n] \oplus E^d(\mathbb{Q})[n].$$

Thus either $E(\mathbb{Q})$ or $E^d(\mathbb{Q})$ has nontrivial n-torsion. If an elliptic curve has n-torsion then it also has an n-isogeny ϕ (where the group generated by the point of order n is the kernel of the n-isogeny), and if an elliptic curve has an n-isogeny, then so does every twist of E. The statement of the lemma follows from these two facts. □

We will also extensively use the well-known classification of possible degrees of cyclic isogenies over $\mathbb{Q}$.

Theorem 6 ([24, 17, 18, 19])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with an n-isogeny. Then $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have complex multiplication, then $n \leq 18$ or $n \in \{21, 25, 37\}$.*

The following four results will be useful in controlling the 2-primary torsion of rational elliptic curves over cubic fields.

Lemma 7 ([31, Lemma 1])**.** *If $E(\mathbb{Q})$ has a nontrivial 2-Sylow subgroup, $E(K)$ has the same 2-Sylow subgroup as $E(\mathbb{Q})$.*

Proposition 8. *Let $M \neq \mathbb{Q}(i)$, and let $E/\mathbb{Q}$ be an elliptic curve such that $E(M)[2] = 0$. Then the 2-Sylow subgroup of $E(L)$ is either trivial or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Proof. Suppose $E(L)[2] \neq 0$. Write

$$E : y^2 = f(x) = x^3 + ax + b,$$

where $f(x)$ is irreducible over M. As L/M is Galois, it follows that since f has one root over L, all the roots of f are defined over M. Hence $E(L)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Suppose that $E(L)$ has a point of order 4. As L does not contain i, it follows that the only possibility for $E(L)$ to have a 4-torsion point is that $E(L)[4] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

We now prove that a group of order 3 has to fix a line of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Let $G := \mathrm{Gal}(L/M)$. We have the short exact sequence

$$0 \to E(L)[2] \to E(L)[4] \to E(L)[4]/E(L)[2] \to 0 \tag{8}$$

and it follows that

$$0 \to E(L)[2]^G \to E(L)[4]^G \to (E(L)[4]/E(L)[2])^G \to H^1(G, E(L)[2]) \tag{9}$$

It is easy to compute that $H^1(G, E(L)[2]) = 0$, and since $E(L)[4]/E(L)[2]$ is a group of order 2, it follows that

$$(E(L)[4]/E(L)[2])^G \simeq \mathbb{Z}/2\mathbb{Z},$$

from which we conclude that $E(L)[4]^G \neq 0$. We conclude that $E(M)$ has a 2-torsion point, which is a contradiction. □

Proposition 9. *Let $M = \mathbb{Q}(i)$. Let $E/\mathbb{Q}$ be an elliptic curve with no $\mathbb{Q}$-rational points of order 2. Then*

a) *If $E(K)$ has a point of order 4, then $\Delta(E) \in -1 \cdot (\mathbb{Q}^*)^2$, $j(E) = -4t^3(t+8)$ for some $t \in \mathbb{Q}$ and $E(L)[4] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*
b) *$E(K)$ has no points of order 8.*

Proof. First note that from the assumption that $E(\mathbb{Q})[2] = 0$, it follows that $E(\mathbb{Q}(i))[2] = 0$. Suppose $E(L)[2] \neq 0$. Since $L/\mathbb{Q}(i)$ is Galois, it follows that $E(L)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

If $E(L)$ has a point of order 4, by the same argument as in the proof of Proposition 8 it follows that $E(L)[4]$ cannot be $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Thus

$$E(L)[4] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},$$

and $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$. Note that for any elliptic curve E', the field $\mathbb{Q}(E'[2])$ contains $\mathbb{Q}(\sqrt{\Delta})$ and $\mathbb{Q}(E'[4])$ contains $\mathbb{Q}(i)$, and since $\mathbb{Q}(E[2])$ is a S_3 extension of E, it follows that Δ is a square in $\mathbb{Q}(i)$, but not in $\mathbb{Q}$, i.e. $\Delta(E) \in -1 \cdot (\mathbb{Q}^*)^2$.

By [6, Lemma], since $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \simeq S_3$, which is isomorphic to a subgroup of $H_{24} = \mathbb{Z}/3\mathbb{Z} \rtimes D_8$, it follows that $j(E) = -4t^3(t+8)$ for some $t \in \mathbb{Q}$. This concludes the proof of a).

Suppose now $E(K)$ has a point of order 8. It follows that $E(L)[8] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Let $G := \mathrm{Gal}(L/M)$ and take the short exact sequence

$$0 \to E(L)[2] \to E(L)[8] \to E(L)[8]/E(L)[2] \to 0. \tag{10}$$

It follows that

$$0 \to E(L)[2]^G \to E(L)[8]^G \to (E(L)[8]/E(L)[2])^G \to H^1(G, E(L)[2]). \tag{11}$$

Note that $E(L)[8]/E(L)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and since we have shown in the proof of Proposition 8 that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ has a G-invariant line, it follows that $(E(L)[8]/E(L)[2])^G \neq 0$. Now from the fact that $H^1(G, E(L)[2]) = 0$ it follows that $E(L)[8]^G \neq 0$, from which it follows $E(M)[2] \neq 0$, which is a contradiction. □

Remark 10. Note that there exist elliptic curves such that $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$ and

$$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \simeq S_3.$$

The elliptic curve 1936D1 is such a curve.

We can combine Propositions 8 and 9 into the following corollary.

Corollary 11. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q})$ has no points of order 4. Then $E(K)$ has no 8-torsion and has a point of order 4 only if $E(K)[2] = 0$, $M = \mathbb{Q}(i)$, $\Delta(E) \in -1 \cdot (\mathbb{Q}^*)^2$, and $j(E) = -4t^3(t+8)$ for some $t \in \mathbb{Q}$.*

Proof. If $E(\mathbb{Q})$ has a 2-torsion point, the statement follows from Lemma 7.

If $E(\mathbb{Q})$ has no 2-torsion, the statement follows from Propositions 8 and 9. □

The next step towards the proof of Theorem 1 is to control the growth of the 3-torsion, for which the following two propositions will be useful.

Lemma 12. *If $E(M)$ does not have a point of order 3, neither does $E(L)$.*

Proof. First note that if an elliptic curve gains points of order 3 over a cubic extension of M, then the 3-division polynomial ψ_3 has to split over M as $\psi_3 = f_1 f_3$, where f_1 is a linear polynomial and f_3 is an irreducible cubic. The torsion points corresponding to f_1 are not L-rational as they are defined over a quadratic extension of M.

Suppose that $E(L)$ has a 3-torsion point. The torsion points corresponding to f_1 are not L-rational as they are defined over a quadratic extension of M, so the only possibility is that $\langle P \rangle = E(L)[3] \simeq \mathbb{Z}/3\mathbb{Z}$. Let $\langle \sigma \rangle = \mathrm{Gal}(L/M)$. As $P^\sigma \neq P$, it follows that the 2 L-rational points of order 3 form an orbit under $\mathrm{Gal}(L/K)$ of length 2, which is impossible by the Orbit Stabilizer Theorem. □

Proposition 13. *Suppose $E(K)$ has a point of order 9. Then $E/\mathbb{Q}$ has an isogeny of degree 9 or 2 independent isogenies of degree 3.*

Proof. Suppose the opposite, that $E/\mathbb{Q}$ does not have an isogeny of degree 9 nor 2 independent isogenies of degree 3. Let $\langle \sigma \rangle = \mathrm{Gal}(L/M)$ and $P \in E(K)$ be a point of order 9. It is easy to see that $E(L)$ has a 9-torsion point, and that $E(\mathbb{Q})$ has a point of order 3 by Lemma 12. Also, $E(M)$ cannot have a point of order 9, since this would imply that $E/\mathbb{Q}$ has a 9-isogeny by Lemma 5, which would contradict our assumption.

We examine how σ acts on P. Let $E[9] = \langle P, Q \rangle$ and $P^\sigma = \alpha P + \beta Q$. If $\beta = 0$, then $\mathrm{Gal}(L/K)$ would fix $\langle P \rangle$, which would imply that $E/\mathbb{Q}$ has a 9-isogeny, contradicting our assumption. Also $P^\sigma \in E(L)$ so $(9-\alpha)P + P^\sigma = \beta Q \in E(L)$, so β has to be 3 or 6, otherwise the full 9-torsion would be defined over L, which would further imply that $L = \mathbb{Q}(\zeta_9)$, which is impossible since $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$. Furthermore, it follows that $E(L)[9] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ and from this $M = \mathbb{Q}(\sqrt{-3})$.

Let $E[3] = \langle P', Q' \rangle$, where $P' \in E(\mathbb{Q})$. Thus $G = \mathrm{Gal}(L/M)$ acts on $\langle Q' \rangle$, and since G is a group of order 3, it follows that $\langle Q' \rangle^G = \langle Q' \rangle$ and hence $E(M)$ has full 3-torsion. By Lemma 5 it follows that $E/\mathbb{Q}$ has 2 independent 3-isogenies, giving a contradiction. □

We now move to the study of the p-torsion of $E(K)$ for $p > 3$.

Lemma 14. *For $p > 3$ prime, $E(L)[p] = 0$ or $\mathbb{Z}/p\mathbb{Z}$.*

Proof. This follows from the fact that $E(L)[p] \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ would, by the Weil pairing, require the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$ to be contained in L, which is impossible. □

Next we study for which p, $E(M)[p] = 0$ implies $E(L)[p] = 0$. We prove a more general statement, that does not apply only for cubic extensions.

Lemma 15. *Let p, q be odd distinct primes, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$, and E/F_1 an elliptic curve with no p-torsion over F_1. Then if q does not divide $p-1$ and $\mathbb{Q}(\zeta_p) \not\subset F_2$, then $E(F_2)[p] = 0$.*

Proof. Since if one point of order p is defined over F_2, then so are all its multiples, it follows that either $p-1$ or p^2-1 points of order p are defined over F_2, but not over F_1. But it is impossible that all p^2-1 appear because of $\mathbb{Q}(\zeta_p) \not\subset F_2$.

Let $\langle\sigma\rangle = \mathrm{Gal}(F_2/F_1)$, P be a point of order p in $E(F_2)$ and then note that $P^\sigma \neq P$, and since $\mathrm{Gal}(F_2/F_1)$ acts on $\langle P\rangle$, it follows that the orbit of P under the action of $\mathrm{Gal}(F_2/F_1)$ has length q, which would imply that $\langle P\rangle$ breaks up into one orbit of length 1 (the identity on $E(F_2)$), and orbits of length q, which is a contradiction, by the Orbit Stabilizer Theorem, with the fact that q does not divide $p-1$. □

In this paper we will use only the special case $q = 3$, $F_1 = M$ and $F_2 = L$ of Lemma 15. We must also be able to show the nonexistence of points of order p^2 in $E(L)$. Again, we prove a more general statement.

Lemma 16. *Let m be a positive integer, p a prime not dividing m, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/p\mathbb{Z}$, E/F_1 an elliptic curve, and suppose $E(F_1) \supset \mathbb{Z}/m\mathbb{Z}$ and $E(F_1) \not\supset \mathbb{Z}/m^2\mathbb{Z}$. Then $E(F_2) \not\supset \mathbb{Z}/m^2\mathbb{Z}$.*

Proof. Suppose the opposite. Let $P \in E(F_1)$ be of order m and $\langle\sigma\rangle = \mathrm{Gal}(F_2/F_1)$. Let

$$S = \{Q \in E(\overline{F_1}) | mQ = P\}.$$

The set S has m^2 elements, on which $\mathrm{Gal}(F_2/F_1)$ acts. By the Orbit Stabilizer Theorem, the orbits under the action of $\mathrm{Gal}(F_2/F_1)$ have to have length p, since if a point in S was left fixed, it would mean that it is F_1-rational. This implies that S decomposes into orbits of p elements each, which is a contradiction with our assumption that p does not divide m. □

We will again use Lemma 16 only in the special case $q = 3$, $F_1 = M$ and $F_2 = L$. For n coprime to 6, the existence of a point of order p in $E(K)$ will imply the existence of an n-isogeny over $\mathbb{Q}$, as the following lemma shows us.

Lemma 17. *Let n be an odd integer not divisible by 3 and suppose $E(K)$ has a point of order n. Then $E/\mathbb{Q}$ has an isogeny of degree n.*

Proof. First note that $E(L)$ has a point P of order n. Let

$$\langle\sigma\rangle = \mathrm{Gal}(L/M),\ \langle\tau\rangle = \mathrm{Gal}(L/K),\ \langle\sigma,\tau\rangle = \mathrm{Gal}(L/\mathbb{Q}).$$

As P is K-rational, it follows that $P^\tau = P$. Let $E[n] = \langle P, Q\rangle$ and $P^\sigma = \alpha P + \beta Q \in E(L)$. But as $(b-\alpha)P + P^\sigma = \beta Q \in E(L)$. It follows that $\beta = 0$ otherwise, $E(L)$ would have full l-torsion, for some $l|n$, which is impossible since L does not contain any lth roots of unity. Hence

$$P^\mu = kP \text{ for all } \mu \in \mathrm{Gal}(L/\mathbb{Q}),$$

and since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\langle P\rangle$ factors through $\mathrm{Gal}(L/\mathbb{Q})$, it follows that

$$P^\mu = kP \text{ for all } \mu \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),$$

which means that $E/\mathbb{Q}$ has an n-isogeny. □

In the special case when $K = L$, the conclusion of Lemma 17 follows when n is a multiple of 3.

Lemma 18. *Suppose $K = L$, i.e. $K/\mathbb{Q}$ is a Galois extension. Let n be an odd integer and suppose $E(K)$ has a point of order n. Then $E/\mathbb{Q}$ has an isogeny of degree n.*

Proof. The proof follows by a similar argument as in Lemma 17 and by using the fact that $\mathbb{Q}(\zeta_k)$ is not contained in K, for any divisor $k \geq 3$ of n. □

5. Proof of Theorem 1

We are now ready to prove Theorem 1, which we will do in a series of Lemmas and Propositions. Recall that if a point in $E(K)$ has prime order p, then $p \leq 13$ (see [33, 34]).

Lemma 19. *The 3-Sylow subgroup of $E(K)$ is isomorphic to a subgroup of $\mathbb{Z}/9\mathbb{Z}$.*

Proof. This follows by [28, Theorem (4.1)] and by the Weil pairing. □

Lemma 20. *$E(K)[5] = E(\mathbb{Q})[5]$ and $E(K)[11] = 0$.*

Proof. By Lemma 15, $E(L)$ has 11-torsion only if $E(M)$ has 11-torsion, which is never true, as rational elliptic curves cannot have 11-torsion over $\mathbb{Q}$ or over a quadratic field, by Theorem 2. Hence $E(K)$ has no 11-torsion.

By Lemma 15 and Lemma 16 and by a similar argument as for the 11-torsion, it follows that $E(L)[5] = E(\mathbb{Q})[5]$ and hence $E(K)[5] = E(\mathbb{Q})[5]$. □

Lemma 21. *$E(K)$ has no points of order 35, 49, 65, 91 or 169.*

Proof. This follows by Lemma 17 and Theorem 6. □

Lemma 22. *There exists no rational elliptic curves with points of order 15 or 16 over a cubic field.*

Proof. As $E(L)[5] = E(M)[5]$ and $E(M)[3] = 0 \Longrightarrow E(L)[3] = 0$ by Lemmas 15 and 12, it follows that the only way for $E(L)$ to have 15-torsion is for $E(M)$ to have 15-torsion.

It follows that, by Theorem 2 c), E is 50B1, 50B2, 50A3 or 450B4. By the division polynomial method, we find that none of these curves have points of order 15 over any cubic field.

If $E(\mathbb{Q})$ has a non-trivial 2-Sylow group, then the 2-Sylow subgroups of $E(\mathbb{Q})$ and $E(K)$ are equal and hence $E(K)$ has no points of order 16. If the 2-Sylow subgroup of $E(\mathbb{Q})$ is trivial, then by Corollary 11, $E(K)$ has no points of order 8. □

Proposition 23. *The elliptic curve* 162B1 *has torsion isomorphic to* $\mathbb{Z}/21\mathbb{Z}$ *over* $\mathbb{Q}(\zeta_9)^+$. *This is the unique pair* (E, K) *of a rational elliptic curve* E *and a cubic field such that* $E(K)$ *has a point of order 21.*

Proof. By Lemma 12, if $E(M)_{tors} = 0,$ or $\mathbb{Z}/7\mathbb{Z}$, then $E(L)[3] = 0$. Suppose now that $E(K)[21] \supset \mathbb{Z}/21\mathbb{Z}$. By Lemma 18, it follows that $E/\mathbb{Q}$ has an isogeny of degree 7, and since it has a 3-torsion point, it also has a 21-isogeny. There are 4 curves (up to $\overline{\mathbb{Q}}$-isomorphism) with a 21-isogeny [27, p.78–80]. These are the curves in the 162B or 162C isogeny classes. Note that the 162B isogeny class is a -3 twist of the 162C class.

By the division polynomial method we find that the only twists of the curves in the 162B and 162C isogeny classes with non-trivial 3-torsion are the curves 162C1, 162C3, 162B1 and 162B3. By the division polynomial method, we find that only 162B1 has a 7-torsion point over a cubic field, the field $\mathbb{Q}(\zeta_9)^+$, which is generated by $x^3 - 3x^2 + 3$. □

Note that since 162B1 is the unique curve with 21-torsion over any cubic field and since it has torsion exactly $\mathbb{Z}/21\mathbb{Z}$, this means that there exist no points of order $21n$ on rational elliptic curves over cubic fields, for any integer $n \geq 2$.

Remark 24. Note that in [31, Remark 2] we misstated that from the fact that

$$X_0(21)(\mathbb{Q}(\zeta_9)^+) = X_0(21)(\mathbb{Q}) \tag{12}$$

(note that $K_7 = \mathbb{Q}(\zeta_9)^+$, using the notation of [31]) one can conclude that there are no elliptic curves with 21-torsion over $\mathbb{Q}(\zeta_9)^+$, while what should have been written is that from (12) we can determine whether 21-torsion appears over $\mathbb{Q}(\zeta_9)^+$ by checking whether twists of rational elliptic curves with rational 21-isogeny have 21-torsion over $\mathbb{Q}(\zeta_9)^+$. The point of the remark, that if we could find out whether $Y_1(25)(\mathbb{Q}(\zeta_9)^+) = \emptyset$, then we could completely classify the possible torsion groups of elliptic curves over $\mathbb{Q}(\zeta_9)^+$, remains true.

Lemma 25. $E(K)$ *does not have points of order* 20, 24, 26, 28, 36 *or* 39.

Proof. Suppose $E(L)$ has a 20-torsion point. Then $E(M)$ has to have a 5-torsion point by Lemma 15,and thus by [21], have a model

$$E : y^2 + (1-t)xy - ty = x^3 - tx^2 \text{ for some } t \in \mathbb{Q}^*. \tag{13}$$

If $E(\mathbb{Q})$ had a 4-torsion point, it would follow that it has a 20-torsion point which is impossible. Thus by Corollary 11, it follows that $E(\mathbb{Q})[4] = 0$ and $\Delta(E) = -k^2$ for some $k \in \mathbb{Q}^*$. Hence

$$-k^2 = \Delta(E) = t^5(t^2 - 11t - 1)$$

for some $t \in \mathbb{Q}^*$, which is equivalent to

$$X : y^2 = t^3 + 11t^2 - t$$

having rational points with $t \in \mathbb{Q}^*$. But $X(\mathbb{Q}) = \{0, (0,0)\}$.

If $E(K)$ had a 24-torsion point then $E(\mathbb{Q})$ would have to have a 8-torsion point by Corollary 11. By Lemma 12, it also has to contain a 3-torsion point and hence a 24-torsion point which is impossible.

Suppose $E(K) \supset \mathbb{Z}/26\mathbb{Z}$. It follows by Lemma 17 that $E/\mathbb{Q}$ has an isogeny of degree 13, and furthermore that $E(\mathbb{Q})[2] = 0$. Since the points of the 13-cycle become rational over K, it follows that K is a splitting field of a polynomial, and hence Galois. It follows that $E(K)$ has full 2-torsion and hence $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$.

By [16, 26] an elliptic curve with a 13-isogeny over $\mathbb{Q}$ has j-invariant

$$j = \frac{(t^2 + 5t + 13)(t^4 + 7t^3 + 20t^2 + 19t + 1)^3}{t}, \ t \in \mathbb{Q}^\times.$$

It follows that E is a quadratic twist of an elliptic curve E_0 with discriminant

$$\Delta(E_0) = t(t^2 + 5t + 13)^2(t^4 + 7t^3 + 20t^2 + 19t + 1)^6(t^2 + 6t + 13)^9$$

$$\times(t^6 + 10t^5 + 46t^4 + 108t^3 + 122t^2 + 38t - 1)^6,$$

and thus $\Delta(E) = u^{12}\Delta(E_0)$ for some $u \in \mathbb{Q}^\times$. The curve E gains full 2-torsion over a cubic field only if $\Delta(E)$ is a square which happens only if

$$X : y^2 = x(x^2 + 6x + 13) \text{ for some } x, y \in \mathbb{Q}^\times$$

has solutions. But $X(\mathbb{Q}) = \{0, (0,0)\}$, and hence that is impossible.

Suppose $E(K)$ has a 28-torsion point. It follows that $E/\mathbb{Q}$ has a 7-isogeny by Lemma 17. If $E(\mathbb{Q})$ had a 4-torsion point, this would imply that $E/\mathbb{Q}$ has a 28-isogeny, which is impossible by Theorem 6. Thus $E(\mathbb{Q})$ does not have a 4-torsion point and by Corollary 11 it follows that L is not a Galois extension of $\mathbb{Q}$ and $\Delta(E) = -k^2$, for some $k \in \mathbb{Q}^*$.

Note that since E cannot have 2 independent rational 7-isogenies, it follows that the kernel of the rational 7-isogeny is equal to $E(K)[7]$. As the

points in the kernel of the rational 7-isogeny are defined over a Galois extension of $\mathbb{Q}$, it follows that they must be defined already over $\mathbb{Q}$, since they cannot be K-rational but not $\mathbb{Q}$-rational (because $K/\mathbb{Q}$ is not Galois).

Hence $E(\mathbb{Q})$ has points of order 7, and by [21], it follows that E is of the form

(14)
$$E : y^2+(-t^2+t+1)xy+(-t^3+t^2)y = x^3+(-t^3+t^2)x^2, \text{ for some } t \in \mathbb{Q}, t \notin \{0,1\}.$$

and that

$$-k^2 = \Delta(E) = t^7(t-1)^7(t^3-8t^2+5t-1),$$

which is equivalent to is a square in $\mathbb{Q}$, which is equivalent to

$$X : y^2 = t(t+1)(t^3+8t^2+5t+1),$$

having rational points such that $t \notin \{0,-1\}$. But the Jacobian J of X has rank 0 over $\mathbb{Q}$ and it is an easy computation in Magma to show that

$$X(\mathbb{Q}) = \{\infty, (0,0), (-1,0)\},$$

and thus completing the proof that there are no rational elliptic curves with 28-torsion over a cubic field.

Suppose $E(K)$ has a 36-torsion point. This implies that $E(K)$ has a 3-torsion point by Lemma 12 and by Corollary 11 either a point of order 4 or no 2-torsion. Also, by Lemma 13, $E/\mathbb{Q}$ has to have a 9-isogeny or 2 independent isogenies of degree 3.

Suppose first that $E(\mathbb{Q})$ has a 4-torsion point, and hence a 12-torsion point. If $E/\mathbb{Q}$ had a 9-isogeny, this would imply that $E/\mathbb{Q}$ is 2-isogenous to a rational curve which has a 36-isogeny, which is impossible by Theorem 6. On the other hand, by [21, Main Result 2.], an elliptic curve with 2 independent 3-isogenies cannot have a 12-torsion point.

Suppose now that $E(\mathbb{Q})$ has no 2-torsion. We split this case into 2 subcases: when $E(\mathbb{Q})$ has a rational 9-isogeny, and when E has 2 independent rational isogenies of degree 3.

Suppose E has a 9-isogeny. Then, by [21, 13], E is a twist of an elliptic curve E_0 with j-invariant

$$j = \frac{t^{12}-72t^9+1728t^6-13824t^3}{t^3-27}, \ t \in \mathbb{Q}\backslash\{0,3\} \tag{15}$$

and

$$\Delta(E_0) = 2985984t^3 - 80621568,$$

and since E has to be a twist of E_0, it follows that $\Delta(E) = u^{12}\Delta(E_0)$, for some $u \in \mathbb{Q}^\times$. By Corollary 11, the curve E gains a 4-torsion point over a cubic field only if $-y^2 = \Delta(E) \neq 0$ has solutions, which is equivalent to

$$X : y^2 = t^3+27, \ t \in \mathbb{Q}\backslash\{0,-3\}, y \in \mathbb{Q}$$

having a solution. But $X(\mathbb{Q}) = \{0, (-3,0)\}$.

Suppose now that E has 2 independent rational 3-isogenies and that E gains a point of order 9 over K. By the same argumentation as in the proof of Proposition 13, it follows that $M = \mathbb{Q}(\sqrt{-3})$. But since E has no rational 4-torsion, but has a 4-torsion point over K, by Corollary 11, it follows that $M = \mathbb{Q}(i)$, which is a contradiction.

If $E(K)$ had a 39-torsion point, this would imply that $E(\mathbb{Q})$ has a 3-torsion point by Lemma 12 and has a 13-isogeny by Lemma 17. But this would imply that $E/\mathbb{Q}$ has a 39-isogeny, which is impossible by Theorem 6. □

Lemma 26. *$E(K)$ cannot have subgroups isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$.*

Proof. Suppose $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. By Lemma 15, this implies that $E(\mathbb{Q})$ has a 5-torsion point. This implies, by [21, Table 3.], that E has a model as in (13). It also follows, since $E(\mathbb{Q})$ cannot contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, that $E(\mathbb{Q})[2] = 0$, and that E gains full 2-torsion over some cubic field. This happens if and only if the discriminant $\Delta(E)$ is a square in $\mathbb{Q}^\times$, i.e. the equation

$$\Delta(E) = y^2 = t^7 - 11t^6 - t^5, \text{ for some } y, t \in \mathbb{Q}^\times$$

has solutions. Dividing out by t^4 and by change of variables we get

$$X : A^2 = t^3 - 11t^2 - t, \text{ for some } A, t \in \mathbb{Q}^\times.$$

The curve X is an elliptic curve and $X(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$, where the rational points are 0 and $(0, 0)$. Thus $E(K) \not\supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Suppose $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. First note that by Lemma 12, $E(\mathbb{Q})$ has a 3-torsion point. Now $E(\mathbb{Q})$ has to either have a 4-torsion point or no 2-torsion by Lemma 7 and Corollary 11.

If $E(\mathbb{Q})$ had a 4-torsion point, then by Lemma 7, $E(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ from which it would follow that $E(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, which is impossible.

If $E(\mathbb{Q})$ had trivial 2-torsion, then $K/\mathbb{Q}$ would have to be a Galois extension for $E(K)$ to have full 2-torsion. But then by Corollary 11, $E(K)$ cannot have points of order 4, which is a contradiction.

Suppose $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$. First note that this implies that $E(\mathbb{Q})$ has a 3-torsion point by Lemma 12. By Lemma 13, $E/\mathbb{Q}$ has either a 9-isogeny or two independent isogenies of degree 3.

Suppose now that $E(\mathbb{Q})$ has a 2-torsion point. Then it follows, by Lemma 7, that $E(\mathbb{Q})$ has full 2-torsion. If $E/\mathbb{Q}$ had a 9-isogeny, this would imply that there exists an elliptic curve with a 36-isogeny over $\mathbb{Q}$, which is impossible. By [21, Proposition III.2.3], an elliptic curve with 2 independent 3-cycles cannot have full 2-torsion. Thus it follows that $E(\mathbb{Q})[2] = 0$ and from this that $K/\mathbb{Q}$ is a Galois extension. Now it follows, by Lemma 18, that $E/\mathbb{Q}$ in fact has a 9-isogeny.

By [21, 13], since E has a 9-isogeny, it is a twist of an elliptic curve E_0 with j-invariant as given in (15) and $\Delta(E_0) = 2985984t^3 - 80621568$, and since E has to be a twist of E_0, it follows that $\Delta(E) = u^{12}\Delta(E_0)$, for some $u \in \mathbb{Q}^\times$. The curve E gains full 2-torsion over a cubic field only if $\Delta(E)$ is a square, which is equivalent to

$$X : y^2 = t^3 - 27,\ t \in \mathbb{Q}\backslash\{0, 3\}, y \in \mathbb{Q}$$

having a solution. But $X(\mathbb{Q}) = \{0, (3, 0)\}$, so there exist no such curves. □

This completes the proof that the groups that appear as torsion groups of rational elliptic curves over cubic fields are contained in the list (4). Note first that by [12, Lemma 3.2 a)], all of the groups from the list (1) appear infinitely often and the group $\mathbb{Z}/21\mathbb{Z}$ has already been dealt with in Proposition 23.

Note that any elliptic curve $E/\mathbb{Q}$ with torsion isomorphic to $\mathbb{Z}/9\mathbb{Z}$ over $\mathbb{Q}$ gains a 2-torsion point over a cubic field K defined by the cubic polynomial $f(x)$, when E is written in short Weierstrass form $E : y^2 = f(x)$. Then by Lemmas 25 and 26 it follows that $E(K)_{tors} \simeq \mathbb{Z}/18\mathbb{Z}$.

It remains to prove, for each of the groups $T = \mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\oplus \mathbb{Z}/14\mathbb{Z}$, that there exist infinitely many elliptic curves E and cubic fields K such that $E(K)_{tors} \simeq T$.

We will deal with the groups $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ simultaneously in the following proposition.

Proposition 27. *There exists infinitely many elliptic curves $E/\mathbb{Q}$ such that there exists a cubic field K over which $E(K)_{tors} \simeq \mathbb{Z}/14\mathbb{Z}$ and there exists infinitely many elliptic curves $E/\mathbb{Q}$ such that there exists a cubic field K over which $E(K)_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$.*

Proof. Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}$. By, [21], this curve has the model as given in (14) If E is written in short Weierstrass form $y^2 = f(x)$, then E gains a point of order 2 over the cubic field K generated by f. We will show that $E(K)_{tors} \simeq \mathbb{Z}/14\mathbb{Z}$. By Lemma 25, $E(K)$ cannot have a point of order 28, so it only remains to show that $E(K)_{tors} \not\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$

If E gained full 2-torsion over K, this would imply that

$$\Delta(E) = t^7(t-1)^7(t^3 - 8t^2 + 5t - 1)$$

is a square in $\mathbb{Q}$, which is equivalent to

$$X : y^2 = t(t-1)(t^3 - 8t^2 + 5t - 1),$$

having rational points such that $t \notin \{0, 1\}$. But the Jacobian J of X has rank 0 over $\mathbb{Q}$ and it is an easy computation in Magma to show that

$$X(\mathbb{Q}) = \{\infty, (0, 0), (1, 0)\},$$

proving the claim.

To prove that there exist infinitely many curves $E/\mathbb{Q}$ such that for each curve there exists a cubic field K such that $E(K)_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$,

we note that every elliptic curve from the infinite family of elliptic curves having torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field from [10, Theorem 4.2] has rational j-invariant. This is a very lengthy but completely straightforward calculation, and hence we leave it out.

The fact that these curves have rational j-invariant does not yet prove that the curves are rational, but just that they are quadratic twists by $\delta \in O_K$ of some rational elliptic curve. We need to prove that in fact δ is rational.

Let E_1 be one of the curves from the family [10, Theorem 4.2] and let E be a rational elliptic curve with the same j-invariant and denote $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$. As already noted $E_1 = E^\delta$. Let $P \in E^\delta(K)$ be a point of order 7. It follows that P^σ is a point of order 7 in $E^{\sigma(\delta)}$ and that P^{σ^2} is a point of order 7 in $E^{\sigma^2(\delta)}$.

Now we will show that in a family of quadratic twists over a cubic field K there can be only one elliptic curve with a point of order 7. Suppose that E_2/K and E_2^d/K are quadratic twists by a $d \in K^\times$ which are not K-isomorphic, and that both have a point of order 7. Then it follows that

$$E_2(K(\sqrt{d}))[7] \simeq E_2(K)[7] \oplus E_2^d(K)[7] \supset \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z},$$

or in other words E has full 7-torsion over $K(\sqrt{d})$. Since $K(\sqrt{d})$ has to contain ζ_7 it follows that $K(\sqrt{d}) = \mathbb{Q}(\zeta_7)$. But elliptic curves over $\mathbb{Q}(\zeta_7)$ cannot have full 7-torsion (see [25]).

Thus it follows that E^δ, $E^{\sigma(\delta)}$ and $E^{\sigma^2(\delta)}$ are all K-isomorphic which means that E^δ is a $\mathbb{Q}$-curve. It is known [7] that $\mathbb{Q}$-curves are either rational or defined over a $(2, \ldots, 2)$ extension of $\mathbb{Q}$. Hence E^δ is defined over $\mathbb{Q}$, completing the proof. □

Remark 28. In the proof of Proposition 27, once we have proven that E^δ, $E^{\sigma(\delta)}$ and $E^{\sigma^2(\delta)}$ are all K-isomorphic, an alternative way of proving that E^δ is rational, without using $\mathbb{Q}$-curves can be done in the following way.

We can see that E^δ, $E^{\sigma(\delta)}$ and $E^{\sigma^2(\delta)}$ are K-isomorphic if and only if

$$\delta\sigma(\delta), \sigma(\delta)\sigma^2(\delta) \text{ and } \delta\sigma^2(\delta)$$

are all squares in K. But since

$$N_{K/\mathbb{Q}}(\delta) = \delta\sigma(\delta)\sigma^2(\delta) = k \in \mathbb{Q},$$

it follows that

$$\delta = ka^2 \text{ for some } k \in \mathbb{Q} \text{ and } a \in K,$$

or in other words that E_1 is a rational twist of $E/\mathbb{Q}$, and hence can be defined over $\mathbb{Q}$.

Note that it is not hard to prove that there exist rational elliptic curves with non-trivial 13-torsion over cubic fields; a short search in Cremona's tables shows that 147B1 is such a curve. The hard part is proving that there are infinitely many such curves. In fact, 147B1 is the only curve with this property that we found in our (short) search.

Let $\{\pm 1\} \leq \Delta \leq (\mathbb{Z}/N\mathbb{Z})^\times$ and define the congruence subgroup

$$\Gamma_\Delta = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) | a \bmod N \in \Delta, N|c \right\}.$$

For N prime, the modular curve $Y_\Delta(N)$ corresponding to Δ has the following moduli space interpretation: a F-rational point on $Y_\Delta(N)$ corresponds to an isomorphism class of pairs $(E, \langle P \rangle)$ of an elliptic curve E/F and a subgroup $\langle P \rangle \in E(\overline{\mathbb{Q}})$ of order N such that every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $\langle P \rangle$ as multiplication by some $\alpha(\sigma) \in \Delta$. Let $X_\Delta(N)$ be the compactification of $Y_\Delta(N)$. Note that if $\Delta = \{\pm 1\}$, then $X_\Delta(N) = X_1(N)$ and if $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times$, then $X_\Delta(N) = X_1(N)$, and that all intermediate curves between $X_1(N)$ and $X_0(N)$ are of the form $X_\Delta(N)$, for some Δ.

We now prove that there are in fact infinitely many rational elliptic curves with non-trivial 13-torsion over some cubic field.

Proposition 29. *There exists infinitely many elliptic curves $E/\mathbb{Q}$ such that there exists a cubic field K such that $E(K)$ has a 13-torsion point.*

Proof. Let $\Delta = \{\pm 1, \pm 3, \pm 4\} \subset (\mathbb{Z}/13\mathbb{Z})^\times$. Then by [9, Theorem 1.1.], $X_\Delta(13)$ has genus 0. As noted above, the elliptic curve 147B1 together with a 13-isogeny, represents a point on $X_\Delta(13)(\mathbb{Q})$ and hence we conclude that $X_\Delta(13)(\mathbb{Q})$ has infinitely many points.

Now let $(E, \langle R \rangle)$, where $E/\mathbb{Q}$ and $\langle R \rangle$ is a 13-cycle of E, be a point on $X_\Delta(13)(\mathbb{Q})$. If every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\langle R \rangle$ by multiplication by an element of $(\mathbb{Z}/13\mathbb{Z})^\times$ of order 3, then it would follow that R is defined over a cubic field and we are done.

Suppose the opposite, that σ acts on $\langle R \rangle$ by multiplication as an element of $(\mathbb{Z}/13\mathbb{Z})^\times$ of order 6. It can be seen, however that when E is written in short Weierstrass form, σ actually permutes the three x-coordinates of $\pm R, \pm 3R$ and $\pm 4R$ and since $x(T) = x(-T)$ for any $T \in E(\overline{\mathbb{Q}})$, this implies that the x coordinates of the points in $\langle R \rangle$ are defined over a cubic field K. Let $F \subset K$ be the field of definition of $\langle R \rangle$. If $F = K$ we are done so suppose $F = K(\sqrt{\delta})$, for some $\delta \in K$. Then $E(F)$ has a point of order 13 and since

$$E(F)[13] = E(K)[13] + E^\delta(K)[13],$$

it follows that either E or E^δ have a K-rational point of order 13. If $E(K)$ has a point of order 13 we are done. Suppose then $E^\delta(K)$ has a point of order 13 and let $\langle \tau \rangle = \mathrm{Gal}(K/\mathbb{Q})$.

Then using the same argument as in the proof of Proposition 27, one can prove that E^δ, $E^{\tau(\delta)}$ and $E^{\tau^2(\delta)}$ all have to be K-isomorphic and hence it follows that E is a $\mathbb{Q}$-curve and it follows that E^δ has to be defined over $\mathbb{Q}$.

Thus for every rational elliptic curve E represented by a point on $X_\Delta(13)$, there exists a rational twist E' such that there exists a cubic field K with the property that $E'(K)$ has a point of order 13. $\square$

6. Sporadic points on $X_1(n)$

As we have seen in Proposition 23, there exists a sporadic point of degree 3 on $X_1(21)$. This point was essentially constructed by starting with an elliptic curve $E/\mathbb{Q}$ with a 21-isogeny and then using the division polynomial method to determine the minimal degree of a field K over which the points in the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant subgroup of order 21 of some twist of E becomes K-rational.

It is a natural question to ask whether the same procedure can be used to find other sporadic points by starting with other rational elliptic curves with isogenies. We have tried this and this method gives us (only) a degree 6 point on $X_1(37)$; we describe the procedure used to find it below.

There are 2 families of twists of elliptic curves with 37-isogenies. We start with the elliptic curve $E = 1225H1$, take a short Weierstrass model

$$y^2 = x^3 - 10395x + 444150$$

of it and factor (over $\mathbb{Q}$) its 37-division polynomial ψ_{37} finding a degree 6 factor

$$f_6 = x^6 - 3150x^5 + 796635x^4 - 75770100x^3 + 3111596775x^2$$
$$-44606598750x - 85333003875.$$

This implies that the x-coordinate of a point of order 37 of E is defined over a sextic field F and since twisting does not change the roots of division polynomials, it follows that there exists an unique twist (over F) of E such that it has a point of order 37 over F. This can be found simply by finding over which quadratic extension $F(\sqrt{\delta})$ the points of order 37 become defined, and then the quadratic twist we are looking for is E^δ. Let w be a root of f_6. We compute that

$$\delta = w^3 - 10395w + 444150$$

and that E^δ indeed has a point of order 37. Thus E^δ, together with a point of order 37 represents a sporadic point of degree 6 on $X_1(37)$, which has gonality 18. Note that this is the same curve which has already been found by van Hoeij [36].

Acknowledgements.

We thank Kestutis Česnavičius for finding a mistake in Proposition 9 in an earlier version and for helping simplify the proofs of Propositions 8 and 9. The author is also grateful to Andrej Dujella and Petra Tadić for helpful comments.

References

[1] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.18 (2012),

[2] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27-49.

[3] P. Clark, P. Corn, S. Lane, A. Rice, J. Stankewicz, N. Walters, S. Winburn and B. Wyser, *Computations on CM elliptic curves*, preprint.
[4] J. Cremona, Algorithms for Modular Elliptic Curves, 2nd ed. Cambridge University Press, Cambridge, 1997.
[5] L. Dieulefait, E. González-Jiménez and J. Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proc. Amer. Math. Soc. **139** (2011), 1961-1969.
[6] T. Dokchitser and V. Dokchitser, *Surjectivity of mod 2^n representations of elliptic curves*, Math. Z. **272** (2012), 961–964.
[7] N. Elkies, *On elliptic K-curves*, Progress in Mathematics 224 (2004), 81–91 (Proceedings of the 7/2002 Barcelona Euroconference on "Modular Curves and Abelian Varieties", ed. J. Cremona, J.-C. Lario, J. Quer, and K. Ribet).
[8] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of* $\mathbb{Q}$, J. Number Theory **114** (2005), 124-134.
[9] D. Jeon, C. H. Kim *On the arithmetic of certain modular curves*, Acta Arith. **130** (2007), 181-193.
[10] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), 579–591.
[11] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), 2395–2410.
[12] D. Jeon, C. H. Kim, A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), 291–301.
[13] P. Ingram, *Diophantine analysis and torsion points on elliptic curves,* Proc. London Math. Soc. **94** (2007), 473–486.
[14] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.
[15] S. Kamienny and F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith. **152** (2012), 291–305.
[16] R. Kloosterman, *Elliptic curves with large Selmer groups*, Master's thesis, University of Groningen, 2001.
[17] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.
[18] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239-244.
[19] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), 415–427.
[20] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
[21] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London. Math. Soc. **33** (1976), 193–237.
[22] M. Laska and M. Lorenz, *Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of* $\mathbb{Q}$, J. Reine Angew. Math. **355** (1985), 163-172.
[23] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186.
[24] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
[25] L. Merel, W. A. Stein, *The field generated by the points of small prime order on an elliptic curve* Internat. Math. Res. Notices **2001**, 1075-1082.
[26] J.-F. Mestre, *La métode des graphes*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields, Katata, 1986.
[27] Modular functions of one variable IV, Edited by B. J. Birch and W. Kuyk. Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin-New York, 1975.
[28] F. Momose, *p-torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **96** (1984), 139-165.

[29] H. H. Müller, H. Ströher and H. G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic fields,* J. Reine Angew. Math. **397** (1989), 100-161.
[30] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory **130** (2010), 1964–1968.
[31] F. Najman, *Torsion of elliptic curves over cubic fields*, J. Number Theory **132** (2012) 26–36.
[32] F. Najman, *Exceptional elliptic curves over quartic fields,* Int. J. Number Theory **8** (2012), 1231–1246.
[33] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier **50** (2000), 723–749.
[34] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Theor. Nombres Bordeaux **15** (2003), 831–838.
[35] A. Pethő, T. Weis and H. G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields*, Internat. J. Algebra Comput. **7** (1997), 353-413.
[36] M. van Hoeij, *Low Degree Places on the Modular Curve* $X_1(N)$, preprint, `http://arxiv.org/abs/1202.4355`
[37] L. Washington, Elliptic Curves. Number Theory and Cryptography, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, 2003.

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: `fnajman@math.hr`